Enabling Mission Assurance Through an Aggressive Critical Infrastructure Protection Program

By Steve Muck

A primary goal of the Department of the Navy's Information Management and Information Technology Strategic Plan is to "protect and defend our Naval critical infrastructures, networks, and information to maximize mission assurance." This article provides an update on how the DON Critical Infrastructure Protection (CIP) program is supporting this goal.

"Mission assurance" is the goal of the Department of the Navy CIP program. Simply put, achieving this goal requires:

(1) Identifying vulnerabilities to assets critical to mission execution;
(2) Remediating such vulnerabilities to protect against possible compromise and, if disrupted by events;
(3) Implementing effective consequence management planning to minimize impact to mission completion; and
(4) Maintaining an active education and outreach effort to proactively institutionalize CIP throughout the Department.

Since its inception more than six years ago, the DON CIP program has developed and implemented policy, processes and products to assist installation commanders/asset owners in improving CIP posture at DON installations worldwide. Current efforts are continuing this strategy as summarized below.

(1) Identifying Critical Asset Vulnerabilities

As the program matured, DON CIP vulnerability assessment protocol expanded beyond Antiterrorism/Force Protection (AT/FP) to include the areas of Computer Network Defense (CND), Commercial Dependency (CD) and Consequence Management (CM) planning — producing a new, improved Naval Integrated Vulnerability Assessment (NIVA). This full spectrum NIVA was conducted at approximately 50 installations over a three-year period, providing a comprehensive snapshot of the current CIP posture to DON commanders and asset owners. As Department of Defense (DoD) and DON policy and guidance evolved, so has the DON CIP team's approach to vulnerability assessments. Current efforts involve the following activities.

Defense Critical Infrastructure Program (DCIP) module assessments to support Chief of Naval Operations IVAs

The assistant secretary of Defense for Homeland Defense (ASD(HD)) disseminated DCIP benchmarks and standards for assessments on critical asset commercial dependencies earlier this year. The resultant "DCIP module" focuses on determining whether significant vulnerability exists in commercial infrastructures that support defense critical assets.

Current DCIP benchmark areas include: energy (electric power, natural gas and petroleum); transportation (roads, rail, aviation, seaports and waterways); water systems (potable, industrial and firefighting); chemical storage and use; heating, ventilation and air conditioning; and communication networks.

The CNO IVA DCIP module focuses on defense owned, leased and managed assets, but its execution also examines commercial providers outside the fence lines of installations.

Navy Reservists and active duty personnel don MCU-2P Chemical, Biological and Radiological (CBR) warfare gas masks during training. U.S. Navy photo.

Opportunities to execute this new approach recently occurred when DON CIP team members conducted DCIP module assessments during the CNO IVAs led by the Naval Criminal Investigative Service at Naval Air Station Oceana in Virginia Beach in July, Naval Air Station Whidbey Island in August and NAS Sigonella, Italy, in September.

Results of these three pilots will be incorporated into next year's CNO IVAs. Feedback from use of the DCIP questions in these assessments is being incorporated into the DON CIP Self-Assessment Tool 2.0.

DON CIP Self-Assessment Tool (SAT)

The ultimate objective of the self-assessment tool is to enable any installation commander/asset owner to perform a critical infrastructure vulnerability assessment at any time. In previous versions, collaboration with DON, DoD, federal and educational entities enabled incorporating best-practice processes and reference materials into a CD-ROM-based CIP self-assessment tool.

This approach has been incorporated into the new, enhanced DON CIP SAT 2.0, which will be accessible via SIPRNET (only) to any installation commander/asset owner.

DON CIP SAT 2.0 incorporates the latest DCIP assessment benchmarks as well as proven best practices with its five-module survey in AT/FP, CND, CD, CM planning, and Chemical, Biological, Radiological, Nuclear and High Yield Explosive (CBRNE) incident response.

For example, questions include whether personnel are trained and equipped for a CBRNE incident. Photos on these pages illustrate types of training.

In addition to the "any time, any place" value, benefits of the DON CIP SAT 2.0 include:

(1) Assessments at a fraction of the cost of current "boots on the ground" protocol;
(2) Broad range of reporting formats;
(3) Consistent, standardized process;
(4) Modular structure that is expandable and easy to keep current; and
(5) One database repository of assessment results with extensive audit and report capabilities.

Development is currently on schedule with completion planned by the end of the first quarter of fiscal year 2007.

(2) Remediating Critical Asset Vulnerabilities

The goal of successful remediation is to achieve maximum return on investment while focusing limited resources on the most essential assets. The Remediation Planning Guide, published in 2004, provides a methodology and plan of action that assists DON entities in developing vulnerability remediation strategies that balance resources and risk.

A new DON CIP effort, Command Remediation Visits, seeks to assist installation commanders in remediating vulnerabilities identified during IVAs. Such remediation visits provide on-site analytical assistance, using the DON Remediation Planning Guide as one tool. For example, the DON CIP team scheduled a Command Remediation Training visit to NAS Whidbey Island to address vulnerabilities identified during its August CNO IVA.

As a direct result of such efforts, ASD(HD) requested support and leadership from the DON CIP team to develop a Remediation Planning Guide suitable for use across DoD. To achieve that goal, an ASD(HD) Remediation Planning Working Group consisting of representatives from the services, Joint Staff, ASD(HD), combatant commanders, and DoD agencies have met to collaborate in developing a DoD-wide guide. Availability of this new planning guide is expected during the first quarter of fiscal year 2007.

(3) Implementing Effective CM Planning

Consequence management planning was added to the NIVA protocol in 2002. CM planning assessments review how well an activity's plans and procedures support its overall continuity of operations. Over the three-year period that NIVAs were conducted, the DON CIP CM team reviewed more than 175 CM plans.

A consequence management planning module has been incorporated into the CIP SAT 2.0 based on the best practices utilized in those assessments as well as the guidance provided in the DON CM Planning Guide, published by the CIP Program in 2003, with an update in 2004.

The DON CM Planning Guide provides methodology and guidance to assist CM planners in developing strategies and plans that will maintain continuity of operations during or after a disruptive event, man-made or act of nature. A working group is evaluating whether the guide should be made mandatory.

(4) Maintaining an Active Education and Outreach Effort

Institutionalizing CIP throughout the DON is a primary goal served by education and outreach efforts. Recent activities in this area include:

School-house training: Incorporating CIP training throughout the Navy and Marine Corps is an integral component of Secretary of the Navy Instruction 3501.1A (CIP) and supports DoD Directive 3020.40 (Defense Critical Infrastructure Program). Since August 2005, more than 390 prospective commanding officers (PCO) of surface ships, submarines, aviation squadrons and shore bases have attended DON "CIP Awareness" briefings.

CIP awareness has been incorporated into the "Commanding Officer Antiterrorism Training" course at the Center for Security Forces (CSF) in Chesapeake, Va.; PCO training at the Surface Warfare Officer School and the Naval War College (NWC) in Newport, R.I.; the Aviation Command Training School in Pensacola, Fla.; and the NWC College of Distance Education "Joint Maritime Operations" course and NWC-Monterey Programs in Norfolk, Va. CIP Awareness has also been presented for one year in the Antiterrorism Officer Course at CSF, adding 330 command antiterrorism officers to those briefed on DON CIP.

Navy Reservists and active duty personnel in an urban warfare training scenario. U.S. Navy photo.

Web-Based DON CIP Program Course: This interactive multimedia suite of instructional courseware defines the DON CIP initiative and the roles and responsibilities of DON personnel in an effective CIP program. The four modules are categorized as Navy Courses DON-CIAO - 5862 - 1, 2, 3, 4 and Marine Corps Courses DI5500A, B, C, D. These courses are available to Department personnel worldwide through the Navy Knowledge Online and the MARINENET portals at http://www.nko.navy.mil and http://www.marinenet.usmc.mil, respectively.

The Way Ahead

The DON CIP program will continue to pursue policy and practice improvements to enhance CIP posture, including: IVA support; self-assessment capability; remediation assistance; consequence management planning guidance; and further institutionalizing CIP throughout the Department.

Contributing to DoD-wide implementation of DON CIP products and tools is another team goal. By continuing to build on achievements made and establishing new objectives to meet tomorrow's warfighting requirements, the DON CIP program will remain focused and effective in enabling mission assurance.

For more information about the ASD(HD) Critical Infrastructure Program go to http://dod-map.msiac.dmso.mil/oasd.htm.

For more information about the DON CIP Program go to http://www.doncio.navy.mil and click on the Project Teams tab, then click on Critical Infrastructure Protection.

Steve Muck is the DON Critical infrastructure Protection team leader. CHIPS